Science and Technology Law Review

Volume 15 | Number 2 Article 8

2012

Killing the Internet to Keep America Alive: The Myths and Realities of the Internet Kill Switch

Scott M. Ruggiero

Killing the Internet to Keep America Alive: The Myths and Realities of the Internet Kill Switch

*Scott M. Ruggiero**

"Congress is debating a kill switch that would allow President Obama to freeze all activity on the Internet if there was a national emergency. The kill switch goes by the top-secret name 'Microsoft Windows.'"

—Conan O' Brien[1]

I. INTRODUCTION

Does the President have the power to shut down the Internet in America? While much debate has centered on a proposed Senate bill that would have given the President an Internet "kill switch,"[2] most Americans would be surprised to discover that the President has had this power for nearly seventy years—decades predating the creation of the Internet. This hot-button issue has resulted in the search of the phrase "Internet kill switch" over 539,000 times on Google.[3]

This paper will discuss the legality and constitutional implications of the "kill switch." Part I will discuss the history and background of the "kill switch." The first section of Part I discusses the law currently in effect. The second section of Part I discusses the Senate's version of Protecting Cyberspace as a National Asset Act of 2010, which provides for the creation of a new office under the executive branch that coordinates cyber security issues with all branches of the federal government and the private sector. The bill allows the President to suspend the Internet on a micro-level in three situations. It has been likened to a scalpel. The third section of Part I describes the changes made to the bill as it was reintroduced in 2011 as the Cybersecurity and Internet Freedom Act. The fourth section of Part I explains the sweeping changes made to the 2011 bill as it has been reintroduced in 2012 as the Cybersecurity Act. Finally, the fifth section of Part I addresses the

---

* Scott M. Ruggiero is a May 2012 Juris Doctorate candidate from Southern Methodist University Dedman School of Law. He is also a 2005 graduate of Florida State University. He would like to thank his coworker Karman Weaver for first asking him if he had heard the story about the Internet "kill switch."

1. Daniel Kurtzman, *The Week's Best Late-Night Jokes*, http://politicalhumor.about.com/b/2011/01/28/the-weeks-best-late-night-jokes-108.htm, ABOUT.COM (Jan. 28, 2011) (quoting Conan O' Brien monologue from *Conan*).

2. *See generally* John Swartz, *Should the Internet have an 'off' switch? Bill gives president power to shut it down during cyberattack*, USA TODAY, Feb. 16, 2011, at 1B. The term "kill switch" is used metaphorically and is not meant to mean that the President actually has a red button on his desk allowing him to either shut off the Internet or launch an all-out nuclear attack.

3. Rebecca Bowe, *CENSORED in a Brave NEW World*, SYRACUSE NEW TIMES Issue 2066, Nov. 3, 2010, *available at* 2010 WLNR 25769252.

Communications Act of 1934. This statute created the FCC, but it also created the sledgehammer—the Internet "kill switch." The switch is not a myth; it is a reality.

Part II of this paper discusses the current law relating to the Internet "kill switch." The first section of Part II discusses the ramifications the legislation has on the freedom of speech. The second section of Part II addresses its effect on the freedom of assembly. Violating freedom of assembly prevents people from assembling to redress some specific grievance they or others have experienced and is an important constitutional liberty.

Part III of this paper discusses the constitutionality of the Internet "kill switch" and examines whether shutting down the Internet is feasible. The recent situation in Egypt has demonstrated, although on a smaller scale, that it is feasible. Part III also examines whether the Protecting Cyberspace as a National Asset Act of 2010 does away with the Internet "kill switch." The legislation does not do away with the "kill switch," but it makes the "kill switch" a more precise instrument when handling targeted cyber attacks. Part III provides reasons against giving the President an Internet "kill switch." This paper also discusses whether the Protecting Cyberspace as a National Asset Act of 2010 is even needed in light of the Communications Act of 1934. I will show that because they are designed with different purposes, both are needed. In addition, Part III hypothesizes how the Supreme Court would rule on the constitutionality of a law that created an Internet "kill switch."

This paper will examine each particular freedom that is infringed by the Internet "kill switch." I demonstrate how this law would eviscerate the freedom of speech and ultimately erode the other First Amendment freedoms. For instance, infringing upon the freedom of speech by preventing people from communicating with each other can ultimately prevent people from organizing together. Hence, it infringes upon the freedom of assembly. Freedom of religion is also violated. This freedom is more difficult to demonstrate as a smaller percentage of people in the United States are reliant upon the Internet as a major source of their religious worship and/or spiritual enrichment. Freedom of the press, like freedom of religion, is limitedly infringed as alternative mediums exist to allow people access to information.

I also examine how the Supreme Court would review a case involving the violation of constitutional liberties caused by the President's use of the Internet "kill switch." This analysis examines the separation of powers of the three branches of government, paying strong attention to Congress's deference to the President regarding matters of national security. This trend has caused the courts to follow in turn. Also, I will examine a Supreme Court decision from World War II that has been widely regarded as erroneous. This case, however, still portrays the thought process of the Supreme Court during wartime. It also demonstrates how the passage of time provides clarity, yet can make a rash decision seem logical during a tumultuous period in history. Finally, I will address why I think an Internet "kill switch" is necessary, but should be limited in scope.

II. HISTORY/BACKGROUND

A. The State of the Current System

During wartime, a great tension exists between liberty and security.[4] The Internet is "an essential element for communication and for operating our financial systems, transportations systems, shipping, electrical power grid, oil and gas pipelines, nuclear plants, water systems, manufacturing, and the military."[5] Internet security has failed to keep pace with the increasing number of Internet users.[6] Some of the money stolen from Internet users through cybercrimes has been funneled to terrorist organizations, which have used the money to fund attacks on the United States and its allies.[7] One negative aspect of cyber espionage is that countries like China can effectively steal valuable military technologies and intellectual property that cost the United States billions of dollars to develop, resulting in the loss of billions in unrealized gains.[8] While it is arguable whether liberty or security deserves more protection, it is agreed that neither should be overlooked nor taken away.[9]

Society is extremely vulnerable in cyberspace due to the global network of interconnected computer networks.[10] "Cyberterrorism" is the term used to describe the "malicious use of cyberspace to cause massive harm to the nation's critical infrastructure."[11] Eighty percent of adults in the United States use the Internet, and there are one billion Internet users worldwide.[12] While the Internet's speed and ease of use has dazzled everyone, these same qualities have left the Internet vulnerable to crime and terrorism.[13] It is logical to assume that since al Qaeda uses the Internet to communicate, the group is probably aware that cyberterrorism can be used as a low-cost and easily concealed means of attack.[14]

---

4. ELIZABETH RINDSKOPF PARKER, CIVIL LIBERTIES IN THE STRUGGLE AGAINST TERROR, *in* LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR 141, 143 (John Norton Moore & Robert F. Turner eds. 2010).

5. S. REP. NO. 111-368, at 1 (2010).

6. *Id.* at 1.

7. *Id.* at 3.

8. *Id.* at 5.

9. John T. Soma et al., *Balance of Privacy vs. Security: A Historical Perspective*, 31 RUTGERS COMPUTER & TECH. L.J. 285, 315 (2005).

10. JEFFREY F. ADDICOTT, CYBERTERRORISM: LEGAL AND POLICY ISSUES, *in* LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR, *supra* note 4, at 519, 519.

11. *Id.*

12. *Id.* at 519–20.

13. *Id.* at 520.

14. *Id.*

There are four general types of cyber attacks.[15] The first and most common type of attack is a service disruption.[16] These types of attacks prevent access to a website and can cause regional or global damage.[17] The second type of cyber attack is one where certain elements of cyberspace are captured and designed to be used as weapons.[18] The third type of attack is when assets are stolen from financial institutions.[19] This attack includes but is not limited to extortion and fraud.[20] The final kind of cyber attack is one in which a physical structure containing electronic industrial control systems that help manage a company's operations is physically destroyed.[21]

Thus far, the government has approached cyber security by cooperating with the private sector but passing no mandatory regulations.[22] Few regulatory laws exist that provide cyber security functions for the private sector.[23] Since the origin of a cyber attack is not immediately known and can come from an amateur, a terrorist, or another nation, the "response baton" will pass from the private sector to law and then to the military.[24]

B. Protecting Cyberspace as a National Asset Act

Congress has attempted to combat the problems associated with cyber attacks over the past several years. In 2010, a cyber-security bill was proposed to the Senate known as the Protecting Cyberspace as a National Asset Act of 2010 (PCNAA or S. 3480).[25] Interestingly, S. 3480 considered cyberspace,[26] a non-tangible medium, to be an asset. The purpose of S. 3480 as

15. ADDICOTT, *supra* note at 528.

16. *Id.*

17. *Id.*

18. *Id.*

19. *Id.*

20. ADDICOTT, *supra* note 4, at 528.

21. *Id.*

22. *Id.* at 542.

23. *Id.*

24. *Id.* at 545.

25. Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. (2010).

26. *Id.* at § 3 (3). "The term 'cyberspace' means the interdependent network of information infrastructure, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." *See also* BLACK'S LAW DICTIONARY (9th ed. 2009). Although "cyberspace" is not explicitly defined by Black's Law Dictionary, "cyberlaw" is defined as law that "addresses issues of online speech and business that arise because of the nature of the medium, including intellectual property rights, free speech, privacy, e-commerce, and safety as well as questions of jurisdiction.

stated in its Senate Report was "to modernize and strengthen the federal government's ability to safeguard the nation from cyber attacks."[27] The primary sponsor of the proposed bill was Senator Joseph Lieberman (ID-CT), with Senators Susan Collins (R-ME) and Thomas Carper (D-DE) as cosponsors.[28]

The bill's authors stated that S. 3480 was needed "to amend the Homeland Security Act of 2002 and other laws to enhance the security and resiliency of the cyber and communications infrastructure of the United States."[29] The Homeland Security and Governmental Affairs Committee Report for PCNAA stated that the Department of Homeland Security needed additional authority not granted to it under the Homeland Security Act of 2002 along with the ability to set risk-based security performance requirements.[30] To facilitate this new authority, S. 3480 envisioned the creation of the National Center for Cybersecurity and Communications (NCCC) under the Department of Homeland Security.[31] In addition to protecting federal computer networks from cyber attacks, the NCCC would also protect "critical infrastructure owned by the private sector" from such attacks.[32] In helping protect private sector networks, the NCCC would work with the private sector in order "to better understand and address the risks our nation faces from cyber threats."[33] The NCCC would be required to share threat, warning, and analysis information with the private sector and other federal agencies as well as provide technical assistance "to help implement best practices, assess vulnerabilities, or otherwise improve the security of cyber networks."[34] By receiving corresponding notifications of vulnerabilities from the private sector, the government would have "situational awareness" of the country's overall cyber security.[35]

In addition to the new NCCC under the Department of Homeland Security, a White House Office of Cyberspace Policy would be created to coordi-

27. S. REP. NO. 111-368, at 1.

28. S. 3480.

29. S. REP. NO. 111-368, at 1.

30. *Id.* at 6. *See also* 6 U.S.C. § 101. The Department of Homeland Security was created under the Homeland Security Act of 2002 and borrows the definition of "critical infrastructure" from 42 U.S.C. § 5195c as "systems of and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

31. *Id.* at 1.

32. *Id.*

33. *Id.* at 6.

34. S. REP. NO. 111-368, at 7.

35. *Id.* at 7–8.

nate with the NCCC and advise the President on cyber security issues.[36] The director of this new office would be appointed by the President and have to be confirmed by the Senate.[37] The director would oversee the cyberspace policies of the military, law enforcement, intelligence agencies, and other diplomatic agencies.[38] The director would also mediate inter-agency disputes.[39]

The hot-button topic of that bill regarded the powers given to the President. The bill would have provided the President with the authority to take limited emergency measures when an entire network shutdown was not necessary.[40] National emergencies warranting protection by the President would include: (1) cyber attacks that would cause damages in excess of $25 billion within a one year period of time, (2) cyber attacks that cause the death of 2500 Americans, or (3) cyber attacks which would force mass evacuations.[41] Covered critical infrastructure[42] could be protected from actual or imminent attack without needing to debate what authority the government has to protect from the attack.[43] Upon notification of a cyber attack that was considered a national emergency, the director would be required to notify the direct owners and operators of all covered infrastructures.[44] The owners and operators would then be required to follow the emergency actions and directions authorized by the Director.[45]

The President's power would be checked by requiring "the President to notify Congress of the threat, why existing security practices are inadequate to mitigate the threat, and what emergency measures are necessary to protect the American public."[46] Emergency measures taken would have to be "the least disruptive" and any measure taken would expire within 30 days unless the President ordered an extension.[47] S. 3480 requires the President to consider not only the affected network but also the broader impact on the nation's information infrastructure.[48] Congressional approval would be

36. *Id.* at 1.

37. *Id.* at 5.

38. *Id.*

39. S. REP. NO. 111-368, at 5.

40. *Id.* at 10.

41. Swartz, *supra* note 2, at 1B.

42. S. REP. NO. 111-368 at 1.

43. *Id.* at 10.

44. S. 3480, 111th Cong. § 249(a)(3).

45. *Id.*

46. S. REP. NO. 111-368, at 11.

47. *Id.*

48. *Id.*

required for any extensions over 120 days.[49] The President would be prohibited from "taking over" any critical infrastructure and ensure that American privacy and civil liberties were protected.[50]

S. 3480 was not signed by the President because he never received the bill.[51] The bill was not placed on the Senate Legislative Calendar under General Orders.[52] While this bill did not reach the President in 2010, it is common for legislators to reintroduce the same bill with the exact or substantially same language in the next legislative term.[53] This bill was reintroduced as the Cybersecurity and Internet Freedom Act of 2011.[54]

C. Cybersecurity and Internet Freedom Act

The Cybersecurity and Internet Freedom Act (Internet Freedom Act or S. 413) was introduced in 2011 by the same authors as S. 3480.[55] S. 3480 was substantially the same as S. 413, but the new bill contained some minor changes.[56] S. 413's stated purpose of amending the Homeland Security Act of 2002 remained the same as did the creation of the Office of Cyberspace Policy and the National Center for Cybersecurity and Communications.[57] The primary difference between the two bills centered on the new bill's explicit admonishment that "neither the President, the Director of the National Center for Cybersecurity and Communications, nor any officer or employee of the Federal Government shall have the authority to shut down the Internet."[58] The proposed bill terminated any powers the President might have under the Communications Act of 1934 discussed *infra*. Finally, S. 413 provided a more straightforward definition of events that would be categorized as regional or national catastrophes.[59] Like the Cyberspace as a National

49. *Id.*

50. *Id.*

51. *S. 3480: Protecting Cyberspace as a National Asset Act of 2010*, http://www.govtrack.us/congress/bill.xpd?bill=s111-3480, (last visited Feb. 14, 2011).

52. *Id.* The lack of a Senate vote on S. 3480 may be attributed to the timing of the bill, and the current economic status of the country. The bill was placed on the Senate's Legislative Calendar on December 15, 2010 near the end of the 2010 term.

53. *Id.*

54. Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011).

55. *Id.*

56. *See id.*

57. *Id.* at §§ 101, 201.

58. *Id.* at § 2(c).

59. Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong., at § 502. According to section 502, the following events constitute a regional or national catastrophe: (I) a mass casualty event which includes an extraordinary

Asset Act, the Internet Freedom Act never made it to the President. A new bill, the Cybersecurity Act of 2012,[60] appears to have taken the Internet Freedom Act's place.

D. Cybersecurity Act of 2012

The Cybersecurity Act of 2012 (Cybersecurity Act or S. 2105) was introduced on February 15, 2012, "to enhance the security and resiliency of the cyber and communications infrastructure of the United States."[61] S. 2105 has kept the National Center for Cybersecurity and Communications from the prior acts while also making significant changes.[62] Most notably, the Cybersecurity Act eliminates the provision in the Internet Freedom Act that prohibits the President from shutting off the Internet. In addition, S. 2105 is silent on the issue of whether the Communications Act of 1934 gives the President the authority to kill the internet during a national emergency. A thorough analysis of this proposed legislation outside the "kill switch" debate is beyond the scope of this paper. The Cybersecurity Act does require cyber risk assessments of designated sectors that operate critical infrastructures.[63] Cyber risks, including those in the private sector, would have to be remediated or mitigated by the owner.[64] This provision has received backlash from some Senate Republicans due to the potentially high costs to the private sector.[65] As a result of election year politics, passage of the Cybersecurity Act is in doubt.[66] Whether a new bill is introduced addressing the President's ability to act under the Communications Act of 1934 remains to be seen.

E. Communications Act of 1934

The Communications Act of 1934 (Communications Act) provides broad powers to the President during times of war, threats of war, or other national emergency. The Communications Act created the Federal Communications Commission (FCC) on national defense grounds and charged it with the task of protecting life and property through the nation's communica-

number of fatalities; (II) severe economic consequences; (III) mass evacuations with a prolonged absence; or (IV) severe degradation of national security capabilities, including intelligence and defense functions.

60. Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012).

61. *Id.*

62. *Id.* at § 242.

63. *Id.* at § 102.

64. *Id.* at § 104(b)(1).

65. Siobhan Gorman, *Cybersecurity Bills Duel Over Rules for Firms*, WALL ST. J., Mar. 9, 2012, at A6, *available at* http://online.wsj.com/article/SB10001424052970203961204577269832774110556.html.

66. *Id.*

tion systems.[67] The Communications Act gives the FCC power to regulate commerce through radio and wire communications.[68] According to Section 706[69] of the Act, the President has the authority to close any facility or station that emits radio communications or wire communications during times of war, threat of war, or some other public peril or disaster if the President deems it necessary for national security and defense purposes.[70] The government also has the power to take over these facilities or stations under these same purposes.[71] The President is not required to provide any prior notice to Congress, and there is no additional check on the President's authority.[72] The creation of the Internet may not have been foreseeable to the legislators who created the FCC because at its inception, only telegraph and telephone services and radio and television broadcasts were included.[73] The FCC is precluded from regulating new technologies unless the new technologies are based off of old technology. Congress may also specifically authorize such regulations.[74]

While the President's unchecked power may seem broad to most, one must look at the historical context in which Section 706 was passed. Section 706 was passed within a month after the Japanese attack on Pearl Harbor.[75] This was a time of unprecedented concern in this country, and Congress passed considerable legislation to help the President defeat the enemies of the United States. Not only has Senator Collins admitted that Section 706 gives the President a "kill switch" to the Internet,[76] but the S. 3480 Senate Commit-

67. *See generally* 47 U.S.C.A. §§151-226 (2011).

68. *Id.* at § 151.

69. Communications Act of 1934, 47 U.S.C.A. § 606 (2011). This section is commonly referred to as Section 706 even though it is found in 47 U.S.C § 606. To avoid confusion, this provision of Act will be referred to as Section 706 throughout.

70. *Id.* at (c)–(d).

71. *Id.*

72. *Id.*

73. Jason Cheek, *Reworking the Emergency Alert System to Meet the Needs of Homeland Security: Overcoming Obstacles to Establish an Effective Public Warning System*, 13 COMMLAW CONSPECTUS 435, 460 (2005).

74. *Id.*; *see also* U.S. v. S.W. Cable Co., 392 U.S. 157 (1968) (finding that the FCC's request to Congress seeking clarification on the FCC's ability to regulate new technologies was not dispositive that the FCC was precluded from regulating the technology).

75. *Protecting Cyberspace as a National Asset Act of 2010: Hearing on S. 3480 Before the S. Comm. on Homeland Sec. & Governmental Affairs* 4, 111th Cong. (2010) (opening statement of Sen. Susan M. Collins, Ranking Member, S. Comm. on Homeland Sec. & Governmental Affairs).

76. *Id.* at 5.

tee Report conceded that Section 706 gives the President the power to shut down an Internet network.[77]

II. CURRENT LAW

In order to gain a proper perspective on the alleged Internet "kill switch", it is important to look at some case law regarding the First Amendment.

A. Freedom of Speech

Of all the constitutional freedoms exhibited by the Internet, perhaps none is more prominent than the First Amendment freedom of speech. "The Constitution gives significant protection from overbroad laws that chill speech within the First Amendment's vast and privileged sphere . . . . As a general principle, the First Amendment bars the government from dictating what we see, read, speak, or hear."[78] The Supreme Court has ruled that speech on the Internet is afforded the same First Amendment protections that newspapers and other publications receive.[79]

Courts have determined that certain types of speech may be restricted despite the First Amendment. Prohibiting speech that is content-based is constitutional only if it is "necessary to serve a compelling state interest and that prohibition is narrowly drawn to achieve that end."[80] Content-neutral speech can be prohibited only if it serves an important or substantial governmental interest, and it must be "narrowly tailored" to address that interest and "leave open ample alternative channels of communication."[81] Examples of unprotected speech include defamation, obscenity, child pornography, and speech that incites violence.[82] The Supreme Court has explained that the government may regulate speech that falls into the above categories because its minimal social value heavily outweighs society's interest in order and morality.[83] The Supreme Court has also stated that some threats of violence also are not protected by the First Amendment.[84]

Courts have read into the First Amendment the right of individuals to speak anonymously.[85] When citizens speak out, they are not required to re-

77. S. REP. NO. 111-368, at 10 (2010).

78. Ashcroft v. Free Speech Coal., 535 U.S. 234, 244–245 (2002).

79. Reno v. ACLU, 521 U.S. 844, 852–53, 868–69 (1997).

80. Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983).

81. *Id.*

82. *Ashcroft*, 535 U.S. at 245–46.

83. R.A.V. v. City of St. Paul, 505 U.S. 377, 382–83 (2002).

84. Watts v. United States, 394 U.S. 705, 707–08 (1969).

85. *See* Watchtower Bible & Tract Soc'y of N.Y. v. Vill. of Stratton, 536 U.S. 150, 166–67 (2002).

veal their identity. This right to anonymity on the Internet is protected so long as the speech does not violate the law.[86] Besides expressing information, the First Amendment "protects the right to receive information and ideas."[87] When guidelines directly impact the right to receive information, courts must analyze them under a heightened scrutiny standard of review.[88] When the regulation does not have a direct impact on the speech, a rational basis standard is applied.[89]

In *Reno v. American Civil Liberties Union*, the plaintiffs filed suit to obtain a preliminary injunction against the Communications Decency Act, which prohibited the transmission of harmful material from the Internet to minors.[90] The Supreme Court distinguished indecent sexual expression from obscene sexual expression and held that sexual expression could not be suppressed merely because it was offensive.[91] The Court further stated that the governmental interest in protecting children from harmful materials did not justify an "unnecessarily broad suppression of speech addressed to adults."[92] In *Doe v. Pulaski County Special School Dist.*, the Eighth Court of Appeals found that a student's letter indicating that he intended to rape and murder a fellow student was not speech that the First Amendment protects, and his subsequent expulsion did not violate the law.[93] In *Clement v. California Dept. of Corrections*, an inmate sought an injunction from a prison policy that prohibited printed materials from the Internet being sent to the prisoners. The Ninth Circuit held that the policy violated his First Amendment right to a freedom of speech.[94] The Court ruled that banning material simply because it was from the Internet was too broad of a purpose.[95] In addition, the Court pointed out that the Supreme Court has stated that inmates retain their First Amendment right to receive information while in prison.[96] Finally, courts have stated that a plaintiff who fails to make a prima facie cause of action

86. *See* Doe v. 2TheMart.com Inc., 140 F. Supp. 2d. 1088, 1092 (W.D. Wash. 2001); Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

87. Stanley v. Georgia, 394 U.S. 557, 564 (1969).

88. Neinast v. Bd. of Trs. of Columbus Metro. Library, 346 F.3d 585, 591–92 (6th Cir. 2003).

89. *Id.* at 592.

90. *Reno*, 521 U.S. at 859–61.

91. *Id.* at 874–75.

92. *Id.* at 875.

93. Doe v. Pulaski Cnty. Special Sch. Dist., 306 F.3d 616, 625–27 (8th Cir. 2002) (en banc).

94. Clement v. Cal. Dep't of Corr., 364 F.3d 1148, 1152 (per curiam).

95. *Id.* at 1153.

96. *Id.* at 1151 (citing Turner v. Safley, 482 U.S. 78, 84 (1987)).

may not force an internet service provider to providing the IP address, thereby protecting the identity of an anonymous website poster.[97]

A recent Supreme Court decision relating to freedom of speech is *Snyder v. Phelps*.[98] The parties asserting the defense of freedom of speech were people who protested at the funerals of soldiers who died serving this country fighting terrorism. The father of Marine Lance Corporal, Matthew Snyder, filed a lawsuit against Phelps and the Westboro Baptist Church for defamation, publicity given to private life, intentional infliction of emotional distress, intrusion upon seclusion, and civil conspiracy. The church had a history of picketing military funerals—picketing nearly 600 funerals over a period of 20 years. The church pickets because it believes that "God hates and punishes the United States" because the American military tolerates homosexuals.[99] Phelps and members of his church crossed state lines and picketed on public land that was adjacent to site of a memorial service honoring Snyder's son. The church notified the police prior to its demonstrations, and none of the church members entered onto the property where the service and the burial were being held. Snyder's father could only see the top of the picketing signs, none of which carried specific remarks relating to his son.[100] Chief Justice Roberts, speaking for a nearly unanimous Court stated that "speech is powerful. It can . . . inflict great pain . . . As a Nation we have chosen . . . to protect even hurtful speech on public issues to ensure that we do not stifle public debate."[101] Thus, the Court held that the church's speech was protected by the First Amendment.[102]

B. Freedom of Assembly

The First Amendment protects both political demonstrations and protests.[103] The police may not interfere with orderly and nonviolent protests simply because they fear public disorder.[104] Assembly at one's own private property usually enjoys stronger First Amendment protections.[105] The stan-

97. *See* USA Technologies, Inc. v. Doe, 713 F. Supp. 2d 901, 908 (N.D. Cal 2010).

98. Snyder v. Phelps, 131 S. Ct. 1207 (2011), *available at* http://www.supremecourt.gov/opinions/10pdf/09-751.pdf, 1.

99. *Id.* at 1.

100. *Id.* at 2. The messages on the signs read as follows: "God Hates the USA/ Thank God for 9/11." "America is Doomed." "Don't Pray for the USA." "Thank God for IEDs." "Thank God for Dead Soldiers." "Pope in Hell." "Priests Rape Boys." "God Hates Fags." "You're Going to Hell." "God Hates You."

101. *Id.* at 15. Only Justice Samuel Alito dissented.

102. *Id.*

103. Boos v. Barry, 485 U.S. 312, 318 (1988).

104. *See* Cox v. Louisiana, 379 U.S. 536, 550 (1965).

105. *See* City of Ladue v. Gilleo, 512 U.S. 43, 58 (1994).

dard for breaking up an assembly is a situation where there is a "clear and present danger of riot, disorder, interference with traffic upon the public streets, or other immediate threat to public safety, peace, or orders."[106] While this section demonstrated the power of the First Amendment, the following section examines whether the President should have an Internet "kill switch" and whether such a device would be constitutional.

III. ANALYSIS

A. Is an Internet "Kill Switch" Feasible?

Before beginning an analysis into whether an Internet "kill switch" would be constitutionally permissible, we must first determine whether it is technologically feasible. An Internet "kill switch" is feasible. In an apparent attempt to try and silence dissent in Egypt, Egypt "unplugged itself entirely from the Internet."[107] Many technologists thought that feat was nearly impossible, considering Egypt's size and major Internet economy.[108] Experts disagree as to whether the Internet could be completely shut off in the United States.[109] Experts have stated that the reason Egypt could effectively shut down the entire country's Internet stems from its centralized government, lack of fiber-optic cables, and strict licenses with the government.[110] Prior to Egypt, Iran limited Internet usage in 2009 when protesters became angered over what they thought were disputed election results.[111]

In some situations, a country's political policies require censorship. For example, China censors much of its own information.[112] China engages in agreements with American companies in which the American companies voluntarily agree to censor searches even though those same searches in the United States would be free of censorship. Yahoo! made such an agreement when it signed the Public Pledge to Self-Discipline for the Chinese's Internet Industry.[113] This pledge prohibits Yahoo! from posting, producing, or dis-

106. Cantwell v. Connecticut, 310 U.S. 296, 308 (1940).

107. Jordan Robertson, *The day part of the Internet died: Egypt goes dark*, WASH. TIMES, Jan. 28, 2011), http://www.washingtontimes.com/news/2011/jan/28/day-part-internet-died-egypt-goes-dark/?page=all#pagebreak (last visited Apr. 2, 2012).

108. *Id.*

109. *Id.*

110. *Id.*

111. *Id.*

112. Kristen Farrell, *Corporate Complicity in the Chinese Censorship Regime: When Freedom of Expression and Profitability Collide*, 11 No. 7 J. INTERNET L. 1, 10 (2008).

113. *Id.* at 11.

seminating information that might jeopardize the socialist culture.[114] Prohibited censoring includes filtering search results and eliminating websites altogether without advising the searcher.[115] Google, which recently challenged China's policy of censorship by refusing to censor Google searches, backed off its original position and agreed to censor searches again.[116]

B. Does the Protecting Cyberspace as a National Asset Act of 2010 Permanently Do Away with the Alleged Internet "Kill Switch?"

The notion that the President might have an Internet "kill switch" has become a topic of much debate.[117] Due to civil unrest as a result of the alleged Internet "kill switch," the Senate Committee on Homeland Security and Governmental Affairs authored two pieces of propaganda designed to alleviate the public's fears.[118] Senator Collins has insisted that the bill would not authorize a "kill switch" for the Internet.[119] What the public appears to be confused about is whether the implementations described in S. 3480 would also apply to Section 706 of the Communications Act of 1934. One author, whose article is reproduced in *What Key Groups and Experts are Saying About the Lieberman, Collins, Carper Cybersecurity Bill*, interprets the S. 3480 as curtailing the power that the President has under Section 706.[120] The text in the Report of the Committee on Homeland Security and Governmental Affairs (Report) says otherwise. According to the Report, S. 3480 ponders whether Section 706 of the Communications Act of 1934, which gives the President the power to shut down an entire network, also allows the President to take smaller, less intrusive action.[121] The Report explicitly indicates that the purpose of S. 3480 is to fill the gap between major

114. *Id.*

115. *Id.*

116. *Google and China Sign New Agreement*, FREEDOMPOLITICS, (July 09, 2010, 9:08 AM), http://www.freedompolitics.com/news/google-1865-href-http.html.

117. *See* Senator Joseph I. Lieberman & Senator Susan M. Collins, *What Key Groups and Experts are Saying About the Lieberman, Collins, Carper Cybersecurity Bill* 11–12, UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS (2010).

118. *Id.*; *see also* Senator Joseph I. Lieberman & Senator Susan M. Collins, *Myth v. Reality The Facts About S. 3480, Protecting Cyberspace as a National Asset* 1, UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS (2010).

119. Adam Cohen, *What's Missing in the Internet Kill-Switch Debate*, TIME (Aug. 11, 2010), http://www.time.com/time/nation/article/0,8599,2009758,00.html.

120. Senator Joseph I. Lieberman & Senator Susan M. Collins, *supra* note 117 at 11 (citing Mickey McCarter, *Protecting Cyberspace Act Gains Momentum*, HOMELAND SECURITY TODAY (June 28, 2010)).

121. S. REP. No.111-368, at 10 (2010).

emergencies requiring the President to use Section 706 and those smaller ones where shutting down an entire network would be overkill.[122] As Senator Lieberman so eloquently puts it, his bill "provides the President with a scalpel . . . so he can *avoid* using the sledgehammer."[123] Thus, the S. 3480 scalpel does not replace the Section 706 sledgehammer. When reading S. 3480, there is no mention that the bill will supersede any part of the Communications Act of 1934. However, as already stated *supra*, the Internet Freedom Act does state that the President is prohibited from shutting down the Internet and may not rely on the Communications Act of 1934. Since the new Cybersecurity Act remains silent on the issue and has been sponsored by the same authors as the PCNAA and the Internet Freedom Act, it is safe to assume that the authors do not wish to limit the President's power under the Communications Act.

C. Reasons Against an Internet "Kill Switch"

Civil libertarians argue that the road to losing constitutional freedoms starts when the government uses national security to restrict rights and liberties.[124] The fundamental complaint about the President's ability to employ an Internet "kill switch" is the deprivation of civil liberties that Americans will experience. These losses consist of the First Amendment freedoms of speech, assembly, religion, and the press.

D. Why the Internet "Kill Switch" Would Infringe on the Freedom of Speech

If the President turns off the Internet, Americans will be deprived of their freedom of speech. This fact is undeniable since the First Amendment explicitly bars the government from dictating what we can say.[125] The Internet contains vast amounts of protected speech including what is posted on websites, message boards, and blogs. While the Internet does contain prohibited speech, such as that which is defamatory, obscene, and incites violence,[126] the Internet primarily contains speech that is not prohibited. Thus, even though the government might have a valid purpose in "protecting individuals from the fear of violence, from the disruption that fear engenders, and from the possibility that the threatened violence will occur," that valid purpose does not apply to situations where *Americans* are under a cyber at-

122. *Id.*

123. *Protecting Cyberspace as a National Asset Act of 2010: Hearing on S. 3480 Before the Sen. Comm. on Homeland Security and Governmental Affairs*, 111th Cong. 4 (2010) [hereinafter *Hearing*] (opening statement Sen. Joseph Lieberman, Chairman).

124. AMITAI ETZIONI, HOW PATRIOTIC IS THE PATRIOT ACT?: FREEDOM VERSUS SECURITY IN THE AGE OF TERRORISM 11 (2004).

125. *See Ashcroft*, 535 U.S. at 244–45.

126. *See id.* at 246.

tack.[127] One of the requirements for regulating content-neutral speech is that the government must leave open alternative channels of communication.[128] Although some may argue that, absent the Internet, there are ample outlets for free speech, the Internet is one of the few avenues that allow for people to express themselves anonymously.[129]

E. Why the Internet "Kill Switch" Would Infringe on the Freedom of Assembly

Another freedom that citizens would lose if the President turned off the Internet is their freedom of assembly. This freedom coincides with the freedom of religion when the Internet is involved. This freedom is somewhat controversial because some might read a "physical" assembly as what the Constitution requires. "If freedom of speech gives people the right to express their viewpoints, freedom of assembly gives people the right to get together and act."[130] One can surmise an Internet freedom of assembly based on a speech given by Secretary of State, Hillary Clinton.[131] According to Secretary Clinton, "the spread of information networks is forming a new nervous system for our planet."[132] Increased access to information and advancements in technology that can open up governments and promote transparency can also be hijacked to crush dissent.[133] Secretary Clinton, speaking on behalf of the Obama administration, stated that the United States "stand[s] for a single internet where all of humanity has equal access to knowledge and ideas."[134]

F. Why the Internet "Kill Switch" Would Infringe on the Freedom of Religion

While freedom of religion does not rely on the Internet, coming together and sharing your faith is part-and-parcel with the universal right of freedom of assembly.[135] This sharing of a common religion may take place online.[136] For instance, one website purports to be an Internet Church—a modern inter-

127. *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 388 (1992) (citing *Watts*, 394 U.S. 705 at 707).

128. *Perry*, 460 U.S. at 45.

129. *See Watchtower*, 536 U.S. at 166–67.

130. Nathaniel Whittemore, *Internet Access is the New Freedom of Assembly*, (Jan. 22, 2010), http://news.change.org/stories/internet-access-is-the-new-freedom-of-assembly.

131. Hillary Clinton, Secretary of State, Remarks on Internet Freedom at The Newseum, Washington D.C. (Jan. 21, 2010) (transcript *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm).

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.*

pretation of the traditional brick and mortar church where visitors from around the world can watch live streaming video of church services from the comfort of their home.[137] In addition to giving users the ability to watch live church services, the website also provides a digital Bible, streaming audio, a chat room, and message boards where users can interact with each other.[138] Another website offers the next best thing—a "live prayer" option whereby a user can simply point-and-click to instantly communicate with someone about his or her prayer needs.[139] Nontraditional churches are not the only churches using online streams. Even some parishes in the Roman Catholic Church offer live streams of Mass and archives of previous sermons.[140]

The Internet allows those who are homebound the opportunity to worship when they would not have the opportunity to do so otherwise. The Internet also facilitates Americans' freedom to worship privately and anonymously. The Internet may also bring together people of different faiths.[141] It is plausible to assume that many Americans have a veiled fear of Muslims simply because Muslim extremists are targeted by the United States for their involvement in the events of 9/11. The key to understanding someone of another faith is knowledge—and the Internet can provide the means for non-Muslims to become familiar with the Islamic faith without having to step foot inside a mosque.

G. Why the Internet "Kill Switch" Would Infringe on the Freedom of the Press

Another freedom citizens may lose with the shutting down of the Internet is their freedom of the press. While not all citizens are professional writers, one commentator has suggested that the line between professional and amateur journalists is becoming blurred.[142] His statement is based on the premise that the special perks and protections afforded to professional jour-

136. Hillary Clinton, Secretary of State, Remarks on Internet Freedom at The Newseum, Washington D.C. (Jan. 21, 2010) (transcript *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm).

137. *Internet Churches Purpose*, ONLINE CHURCHES, http://internet-churches.com/purpose.htm (last visited Mar. 3, 2011).

138. *Id* (stating that The Online Church is an alternative to the "traditional" church and is meant for "drop outs" from institutionalized churches, those that are homebound and cannot physically be at church, those people fed up with "multi-layered" churches that focus more on money and less on God, busy individuals who need a flexible schedule for attending church, and non-Christians desiring the opportunity to examine the claims of Christ).

139. LIFECHURCH, http://live.lifechurch.tv/ (last visited Mar. 3, 2011).

140. *Live Streaming Mass & Archive*, St. Anne Roman Catholic Parish, Gilbert, Ariz. http://www.stanneaz.com/stanne/ (last visited Mar. 3, 2011).

141. Clinton, *supra* note 131.

142. *See* SCOTT GANT, WE'RE ALL JOURNALISTS NOW 5 (2007).

nalists should be offered to others since the First Amendment is for all citizens.[143] Thousands of blogs exist where nonprofessional journalists report, analyze, and provide opinions on a variety of issues.[144] These blogs exist because computers have become inexpensive, more powerful, and software enables the easy sharing of information and opinions with a worldwide audience.[145]

A significant change in mainstream media has resulted due to changes in traditional news reporting.[146] While traditional print media has limited itself due to financial constraints, citizen journalism has emerged to fill the void.[147] A perfect example is the amateur videos and commentary from those people who remained in New Orleans and rode out Hurricane Katrina.[148] Even established news networks like ABC, CBS, and NBC solicit video and eyewitness accounts from citizens.[149] A California court of appeals has impliedly stated that a website that disseminated information taken from Apple did not have to disclose the identities of the employees who provided the information.[150] The court stated that because the information provided by Apple employees was newsworthy and came within the scope of the First Amendment, the website owner was precluded from having to give up the identities of the anonymous employees.[151]

H. Citizens Will Not Have Enough Information to Make Informed Decisions About Potential Deprivations of their Constitutional Liberties

Informed decisions can only be made if you have information. Citizens are more inclined to tolerate a restriction on civil liberties when there is a greater distinction between "us" and "them."[152] That is, when a national threat is attributed to a clearly identifiable group or entity, the public is more willing to confer upon the government emergency powers.[153] In acknowledging that the public would be more understanding of the government as-

143. *Id.* at 5.

144. *Id.* at 26.

145. *Id.* at 6.

146. *Id.* at 137.

147. GANT, WE'RE ALL JOURNALISTS NOW 138 (2007).

148. *Id.* at 138.

149. *Id.* at 139.

150. O'Grady v. Super. Ct. of Santa Clara Cnty., 44 Cal. Rptr. 3d 72, 115 (6th Dist. Ct. App. 2006).

151. *See id.*

152. Oren Gross, *Chaos and Rules: Should Responses to Violent Crises Always be Constitutional*, 112 YALE L.J. 1011, 1037 (2003).

153. *Id.*

suming greater powers during a national crisis, it is important to remember that in a cyber attack, we may not necessarily know "them."[154]

I. Why Problems are Created When the Government Tries to Balance Liberty with Security

Another reason why the President should not have an Internet "kill switch" is that problems are created when the government tries to balance liberty with its security goals. A prime example of this would be the "No Fly List."[155] You may recall that the "No Fly List" was a list provided by the government to the airlines that effectively prevented anyone on the list from flying on a commercial airliner. Unfortunately, several anti-war demonstrators and prominent Democrats had their names unwittingly placed on that list.[156] "These actions raised questions as to what response would be appropriate to restore citizen confidence when well-motivated government employees mistakenly collect personal information as part of an effort to warn and protect against further terrorist attacks."[157] It is important for the President to remember that "the ultimate source of oversight is the citizenry, informed and alerted by a free press and civil liberties advocates and briefed by public authorities about their needs."[158]

J. Is the Protecting Cyberspace as a National Asset Act of 2010 or a Similar Bill Necessary?

Senator Lieberman has provided this cryptic message about a cyber-attack:

> Given our nation's reliance on the Internet to run our most critical infrastructure, the potential damage from a concerted cyber attack is equal to, if not greater than, what we might experience from a conventional military attack on our homeland. A full-scale cyber attack could turn off our electricity and all that we run on it; it could cause generators to burn out, pipelines to explode, and dams to fail and could lead to the death and injury of thousands of people, and could cost our economy billions of dollars. This is no longer fantasy or fiction. It is a clear and present danger.[159]

---

154. *Id.*

155. ELIZABETH RINDSKOPF PARKER, CIVIL LIBERTIES IN THE STRUGGLE AGAINST TERROR, *in* LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR, *supra* note 4, 141, 164–65.

156. *Id.* at 164.

157. *Id.* at 164-65.

158. ETZIONI, *supra* note 124, at 72.

159. *Hearing*, *supra* note 123, at 1.

During national emergencies, the President needs a quick and effective way to safeguard our nation from cyber attacks. The Protecting Cyberspace as a National Asset Act (PCNAA), or a bill like it, would give the President the ability to make surgical shutdowns of certain portions of the Internet without infringing on the constitutional liberties of *all* Americans. Further, requiring the President to notify Congress of the reasons for a continuous shutdown of certain suspect websites would provide the nation with the system of checks and balances required in the Constitution.

An Internet "kill switch" and a bill like the Protecting Cyberspace as a National Asset Act of 2010 is necessary because of the lack of sharing on the part of U.S. companies. Private companies are usually unwilling to share information about security breaches with the government or other companies.[160] The primary reason that companies are unwilling to share information is that they are concerned with proprietary information that has been shared with the government and may be available to other companies through the Freedom of Information Act.[161] Second, the revelation of security breaches to the public could have adverse effects on the company and its stockholders.[162]

The major problem with the proposed PCNAA bill is the limit of civil liability on designated covered entities. According to the bill, covered entities would not be liable for noneconomic or punitive damages as long as certain requirements had been met.[163] The problem is that most of the requirements have to be met by the government rather than the covered entities. For example, the covered entities are immune if the President issues a declaration of a national cyber emergency, the Director issues emergency measures as a result of the President's declaration, and the Director then certifies to the court that actions taken by the entity in response to the *Director's* orders were in compliance.[164] The only damages the covered entity could be liable for are those that cause physical injury or death or substantial damage or destruction to a person's primary residence.[165]

American corporations' involvement in bills like the PCNAA is noticeable. That bill provided that the United States shall defend and indemnify covered entities.[166] It should be noted that computer companies such as Google, Verizon, and AT&T spent considerable sums lobbying for the pro-

160. ADDICOTT, *supra* note 10, at 547.

161. ADDICOTT, *supra* note 10, at 547.

162. ADDICOTT, *supra* note 10, at 547.

163. *See* S. 3480, 112th Cong. § 249 (e) (2010).

164. *Id.* at (4).

165. *Id.* at (5)(I)–(II).

166. *Id.* at (5)(D).

posed bill.[167] Assuming the courts found that there were, in fact, constitutional violations, the American people would most likely sue the corporations with deep pockets rather than the United States. The multiple provisions in the bill limiting civil liability and providing for government indemnity are concerning because the American people do not appear to have much, if any, ability to recover for violations of their constitutional freedoms. Although this type of bill is needed to give the President a "scalpel" rather than having to resort to using the "sledgehammer" of the Internet "kill switch," these provisions in the bill should be removed.

K. How the Supreme Court would Rule on the Internet "Kill Switch"

Given standing requirements, it is likely that the Supreme Court would rule on the Internet "kill switch" or the scalpel effect of a bill like the Protecting Cyberspace as a National Asset Act of 2010 *after* the President had already employed the measures. Perhaps the biggest hurdle the President would face in a lawsuit concerning the Internet "kill switch" is a separation of powers argument. Historically, the Supreme Court has shown deference to Congress when it grants the President powers not specifically mentioned in the Constitution. Congress has also shown historical deference to the President on matters of diplomacy, intelligence, and war.[168] This deference towards the President would likely continue even though the terms "national security" and "foreign affairs" are not mentioned in the U.S. Constitution.[169] This national security tension takes on an ebb and flow approach whereby executive and legislative reaction subsides as the crisis reduces.[170] Once the emergency has subsided, the judicial branch re-evaluates the prior risks, and reigns in the other two branches according the court's interpretations of constitutionally guaranteed rights.[171]

Here the Court could consider the information imbalance between the executive and legislative branches. Opponents of the Internet "kill switch" would argue that by allowing the executive branch to unilaterally control access to information on the Internet in times of a national emergency, Congress would create an "executive monopoly" that is damaging to our democ-

167. *See Lobbying Report Google Inc., available at* http://disclosures.house.gov/ld/pdfform.aspx?id=300303950; *Lobbying Report Verizon Communications Inc., available at* http://disclosures.house.gov/ld/pdfform.aspx?id=300299882; *Lobbying Report AT&T Services, Inc., available at http://disclosures.house.gov/ld/pdfform.aspx?id=300302527.*

168. ROBERT F. TURNER, U.S. CONSTITUTIONAL ISSUES IN THE AGAINST TERROR, *in* LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR, *supra* note 4, at 81, 82.

169. *Id.*

170. *Id.* at 143.

171. *Id.*

racy.[172] Additionally, they contend that the executive branch does not have exclusive knowledge when it comes to matters of national security.[173] Congress, through its various committees on military, foreign policy, and intelligence matters is also knowledgeable about matters of national security.[174]

A review of some post-9/11 cases may be indicative of how the Court would rule. In *Hamdi v. Rumsfeld*, an American citizen had been detained by the government for his alleged connections to the Taliban.[175] His father sought a petition for habeas corpus for his son on the grounds that as an American citizen, he should have access to legal counsel and be provided notice of the charges against him, neither of which had been done.[176] The Court did not reach the issue of whether the President had the authority under the Constitution to hold Hamdi, but the Court stated that Congress had expressly given the President these powers under the Authorization to Use Military Force statute ("AUMF").[177] From this case, it can be inferred that the Court will duck the issue of whether the President has implied power if the Court can find Congressional authorization granting the same powers.

In *Hamdan v. Rumsfeld*, President Bush indicated that alien enemy combatants would be tried under military tribunals pursuant to the President's Commander-in-Chief powers and the AUMF.[178] Hamdan was an alien enemy combatant who was transferred to Guantanamo Bay after having been held in Afghanistan.[179] After a year in Guantanamo, he was deemed eligible for trial by a military commission that had not been expressly authorized by Congress.[180] A year later he was charged with conspiracy, and he eventually petitioned for a writ of habeas corpus.[181] The issue in the case was whether the President had the authority to create military tribunals *without* congressional authorization.[182] The Court held that the President did not have the authority to create military tribunals by executive order without congres-

172. Stephen J. Schulhofer, *Secrecy and Democracy: Who Controls Information in the National Security State?*, NEW YORK UNIVERSITY PUBLIC LAW AND LEGAL THEORY WORKING PAPERS, PAPER 217, at 3 (2010), *available at* http://lsr.nellco.org/nyu_plltwp/217 (last visited Apr. 1, 2011).

173. *Id.*

174. *Id.*

175. Hamdi v. Rumsfeld, 542 U.S. 507, 510 (2004).

176. *Id.* at 511.

177. *Id.* at 516–17.

178. *See* Hamdan v. Rumsfeld, 548 U.S. 557, 558–59 (2006).

179. *Id.* at 566.

180. *Id.*

181. *Id.* at 566–67.

182. *Id.* at 572.

sional authorization.[183] Even though the Court did not rule in the President's favor in this case, it falls in line with the theory that congressional approval of presidential action seems to meet the prerequisite of constitutionality.

Proponents for strict separation of powers would argue that the Framers did not want to give the President exclusive powers over declaring states of emergency.[184] Professor Scheppele states that the most persuasive argument in interpreting the Framers' intent of why they did not want national emergency powers to be provided solely to the President is that Congress alone was given the power to declare war.[185] An additional reason provided by Scheppele supporting this same proposition is that the Constitution gave Congress the power to quarter troops only in times of war as long as that law had been previously passed.[186]

Professor Schulhofer states that presidents can be inclined to violate the Constitution when they believe the good of the nation requires it.[187] In fact, Thomas Jefferson stated that "every good officer must be ready to risk himself in going beyond the strict lines of law when the public preservation requires it."[188] Interestingly, Jefferson does not indicate that the President should get a free pass in violating constitutional liberties, and one may infer that he believes a president may be impeached for doing so. For Jefferson though, it seems that sacrificing your career for the good of the country is a price any true patriot would be willing to pay.[189]

The ultimate question then is how would the Court rule? Based on the Supreme Court's history, the Court would probably rule in favor of both the Internet "kill switch" and a bill similar to the Protecting Cyberspace as a National Asset Act of 2010. Before the terrorist attacks on September 11, any proposal by the United States government to eliminate hate speech in the interest of national security would have been considered unnecessary, unwise, and probably unconstitutional.[190] Unfortunately for civil libertarians, September 11, 2001, is a date that changed the public perception as to these rights. Even though "our current free-speech jurisprudence simply does not accept . . . a rationale for restricting otherwise protected speech," a declaration of a national emergency due to a cyber attack would restrict protected

183. *Id.* at 613.

184. Kim Lane Scheppele, *Law in a Time of Emergency*, SCHOLARSHIP AT PENN LAW Paper 55, 5-6, *available at* http://lsr.nellco.org/upenn_wps/55 (Mar. 4, 2004).

185. *Id.* at 5.

186. *Id.*

187. *See* Schulhofer, *supra* note 171, at 6.

188. *Id.*

189. *See id.*

190. ROBERT M. O'NEIL, HATE PROPAGANDA AND NATIONAL SECURITY, *in* LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR, *supra* note 4, at 171, 171.

speech for the overall good of the country.[191] Professor Schulhofer argues that legislative and judicial checks can be ineffective because the executive branch often refuses to share all material information to Congress and the courts.[192] With the Court showing such deference to the President and Congress in matters of national security, it is reasonable to assume that the Court would find in favor of the President, especially if the Court is purposely kept in the dark.

Although the Court will likely balance the risks versus the benefits of infringing one's constitutional liberties, the Court will be highly concerned with the imminence of the threat likely weigh heavily in favor of eliminating the threat.[193] This belief is based on the premise that during times of grave national crises, protection of human rights and civil liberties is pushed to the side until the crisis is over.[194] In addition, we must remember that judges are human beings. As Professor Oren Gross opines, the courts are highly deferential to executive and congressional actions because, like citizens in general, judges want to win wars.[195]

The most persuasive case as to why the Supreme Court would rule in favor of the constitutionality of both the Internet "kill switch" and a bill like the Protecting Cyberspace as a National Asset Act of 2010 comes from the Supreme Court case of *Korematsu v. United States*.[196] Though the legal community considers this an appalling decision by the Court, it exemplifies the type of decision-making when this country is at war. This case involved Executive Order No. 9066, which was signed in 1942.[197] This order authorized military commanders to set aside certain exclusionary areas where persons of Japanese ancestry, if found in that area, would be subject to criminal penalties.[198] Congress later enacted legislation that made it a crime to violate this order.[199] A western military commander later ordered a curfew for Japanese Americans living on the West Coast.[200] The Supreme Court held this curfew to be constitutional in the case of *Hirabayashi v. United States*.[201]

191. *Id.* at 191.

192. Schulhofer, *supra* note 171, at 5.

193. Gross, *supra* note 152, at 1038.

194. Gross, *supra* note 152, at 1034.

195. Gross, *supra* note 152, at 1034.

196. Korematsu v. United States, 323 U.S. 214 (1944).

197. *Id.* at 217.

198. *Id.* at 220.

199. *Id.* at 216.

200. *Id.* at 217.

201. Hirabayashi v. United States, 320 U.S. 81, 92 (1943) (holding that applying the curfew order to the entire group was constitutional because it would be impossible to bring about an immediate desegregation of the loyal from the disloyal).

The military later ordered the Japanese living on the West Coast to stay in "Assembly Centers" or "Relocation Centers."[202] These camps were similar to the concentration camps in which the Nazis imprisoned the Jews, with the exception that the United States government did not brutally murder the inhabitants. Korematsu was a U.S. citizen that had unquestioned loyalty and who was tried and convicted of refusing to leave his property.[203] In ruling against Korematsu, the Court stated:

We cannot reject as unfounded the judgment of the military authorities and of Congress that there were disloyal members of that population, whose number and strength could not be precisely and quickly ascertained. We cannot say that the war-making branches of the Government did not have ground for believing that in a critical hour such persons could not readily be isolated and separately dealt with, and constituted a menace to the national defense and safety, which demanded that prompt and adequate measures be taken to guard against it.[204]

Justice Jackson, who issued a harsh dissent, stated that "if we cannot confine military expedients by the Constitution, neither would I distort the Constitution to approve all that the military may deem expedient."[205]

One interesting way to distinguish *Korematsu* from the present case where the President would authorize a total or partial shut down of the Internet is the level of public awareness—the Japanese-Americans' detainment was much more widely known.[206] Returning to Jefferson's "public preservation" mentioned *supra*, public emergencies by their very nature are not always visible to the public because the government is able to conceal them.[207] The government could easily shut down a website site due to a cyber attack without mentioning it to the American people, with people finding out only when the website fails to load.

Given the Supreme Court's recent decision in *Snyder v. Phelps*, it may seem that the Court is fundamentally concerned with infringing citizens' freedom of speech.[208] In that case, the Court protected took pains to protect invidious speech. It is reasonable to conclude that the Court would be unwilling to allow government suspension of all citizen speech in the event of a cyber attack. Another recent Supreme Court decision also written by Chief Justice John Roberts less than a year before *Snyder v. Phelps* indicates that

202. *Korematsu*, 323 U.S. at 220–21.

203. *Id.* at 221, 223.

204. *Id.* at 218.

205. *Id.* at 244 (Jackson, J., dissenting).

206. *See* Schulhofer, *supra* note 171, at 6.

207. Schulhofer, *supra* note 180, at 6.

208. *See* Snyder v. Phelps 131 S. Ct. 1207, 1220 (2010) (noting the Court found that the Westboro Church had the right to picket military funerals).

speech concerning terrorist organizations is not protected.[209] In *Holder v. Humanitarian Law Project*, six domestic organizations initiated a constitutional challenge to the material support statute, which prevents U.S. citizens and organizations from materially supporting organizations the government has designated as terrorist in nature.[210] The organizations sought to provide material support to two terrorist organizations, the Partiya Karkeran Kurdistan ("PKK") and the Liberation Tigers of Eelam ("LTTE").[211] The organizations claimed that by providing material support in the form of speech only to the humanitarian portions of the terrorist groups, they would be protected by the First Amendment's freedom of speech and not be in violation of the statute.[212] The Court found that the First Amendment did not protect the organizations because providing material support in any form to terrorist organizations would undermine cooperative efforts between the U.S. and other nations fighting terrorism.[213] Thus, while free speech is important in the domestic context, the Court has given notice that even peaceable speech is not protected when terrorist organizations are involved.

L. The WikiLeaks Problem

An interesting hypothetical to add to the debate on the internet "kill switch" is whether the leaked documents from WikiLeaks would qualify as a national emergency necessitating a presidential response. At least 92,000 documents have been leaked about the United States' War in Afghanistan.[214] WikiLeaks is a private international organization that is based in Sweden.[215] The White House and the military have not questioned the legitimacy of the documents released.[216] According to the White House, the release of the information poses a significant national security risk.[217]

Whether WikiLeaks would be considered a national security emergency depends on the extent of the damages caused by the release of the informa-

209. Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2731 (2010).

210. *Id.* at 2713–14.

211. *Id.* at 2714 (noting the PKK aims to establish an independent state in Turkey, while the LTTE seeks to do the same in Sri Lanka. Both organizations carry out political and humanitarian activities, but our government has classified them as terrorists due to multiple attacks, some of which harmed Americans).

212. *See id.*

213. *Id.* at 2726.

214. Ryan Witt, *A Summary of the Most Significant WikiLeaks Documents from the War in Afghanistan*, EXAMINER, Mar. 4, 2011, http://www.examiner.com/political-buzz-in-national/a-summary-of-the-most-significant-wikileaks-documents-from-the-war-afghanistan.

215. *Id.*

216. *Id.*

217. *Id.*

tion. Per the Communications Act of 1934, the release of the information might be sufficient to cause the President to activate the internet "kill switch." The inherent problem with using the switch as referenced herein is that it would shut down the entire Internet rather than solely targeting WikiLeaks.

PCNAA addressed this very issue—the bill advocates using the scalpel approach rather than a sledgehammer. The problem with the PCNAA in its current form is that, in order to utilize its provisions, the president would be required to show mass evacuations and billions of damages in a one-year period. On its face, WikiLeaks would not adhere to any of the aforementioned stipulations. WikiLeaks will not likely cause mass evacuations. Presumably, if WikiLeaks is releasing strategic military plans, this could allow an enemy of the United States to take advantage of this opportunity to strike against the United States' military. As of this writing, the military claims that the released information was old information from the Bush administration, and the Obama administration has since revised their military strategy in Afghanistan.[218] Although no new information has been released, there is nothing preventing WikiLeaks from releasing current military data. If, however, the President engages a scalpel-like method on WikiLeaks, how precise will the cut be? Although most Americans would seemingly support suppressing national security information, they likely would not favor suppressing data that could potentially expose government corruption and waste.

As to the issue of damages, these would be difficult to quantify. It could be argued that there would be no monetary damages because release of information is hardly considered a cyber attack and national infrastructure would not be damaged. However, the cost associated with preventing and monitoring data to ensure it is not leaked could potentially cost billions. Further, if military operations which have been in practice for years become compromised, the restructuring of these operations could prove costly.

Since Congress defers to the President on matters of national security, it is highly unlikely that Congress would question him. Even so, the amount of time the President has to carry out his mission of thwarting a cyber attack may be more than ample to cause a permanent end to WikiLeaks. Justice Sotomayor has mentioned that WikiLeaks could influence future Supreme Court cases involving the First Amendment.[219]

---

218. *Id.*

219. *See* Kurt Nimmo, *Sotamayor Says Court May Rule to Limit First Amendment in Response to WikiLeaks*, INFOWARS, Aug. 28, 2010, http://www.infowars.com/sotomayor-says-court-may-rule-to-limit-first-amendment-in-response-to-wikileaks/ (commenting on the answer Justice Sotomayor gave responding to a student's question at a speech she gave at the University of Denver. Sotomayor stated, "that was not the beginning of the question, but an issue that keeps arising from generation to generation, of how far we will permit government restriction on freedom of speech in favor of protection of the country.").

IV. CONCLUSION

The Internet "kill switch" is a reality. As pointed out herein, Section 706 of the Communications Act of 1934 provides the President with the broad power to shut down or takeover any wire or other communication facility.[220] This power has been likened to a sledgehammer. The Protecting Cyberspace as a National Asset Act of 2010, or a similar bill, would give the President the authority to minimize the damaging effects of the Section 706 sledgehammer by performing smaller, surgical repairs to critical infrastructures. It would also create a new White House Office of Cyberspace Policy with a presidential-appointed and Senate-confirmed director tasked with coordinating cybersecurity with both federal agencies and the private sector.[221] The bill would require the President to inform Congress of his reasons for employing the measures in S. 3480 and would limit him with timetables unless he received extensions from Congress.[222]

One concern over the bill is that there is no discussion of what would happen if Congress did not initially agree that the measures needed to be taken.[223] Another concern regarding the bill is that First Amendment freedoms would be infringed if either the internet "kill switch" or the Senate bill is utilized by the President. The freedom of speech is the fountainhead of the other freedoms. Therefore, this freedom will be the one most violated by this action. Freedom of assembly will be violated because preventing people from speaking online also prevents them from assembling. Case in point, the recent situation in Egypt in which President Mubarak attempted to prevent his people from assembling by shutting down Facebook. The same holds true for freedom of religion. Homebound individuals will have no method of worshipping their God without access to the Internet. Although the elderly and handicapped once were unable to practice their religion due to their isolating situation, the Internet has now provided a new mode of worship. In addition, freedom of the press would be violated because many people get their news and information from the Internet. This can be seen in the way the Internet has extinguished the need for print media such as newspapers.

Although the alleged Internet "kill switch" can become a reality under our current laws, the President should take great care to avoid using it. This power is a necessary evil of our democracy. Based on precedent, the Supreme Court would most likely find that when confronted with an impending national cyber attack that could kill thousands and cost billions, the scales would tip in favor of suspending constitutional liberties. Events like the bombing of Pearl Harbor and the attacks on September 11, 2001, are likely to happen again sometime in the future. Faced with uncertainty and paranoia, this country has reacted with gut reactions that have infringed the constitu-

220. *See* 47 U.S.C. § 606 (c)–(d) (1934).

221. S. REP. No. 111-368, at 1 (2010).

222. *Id.* at 11.

223. *See id.*

tional liberties of our fellow citizens. The Supreme Court has reacted to these paranoid times by ruling with its heart and not with its head. This is quite evident when you consider how the United States government later paid reparations to Japanese-Americans who had been detained during World War II. Regardless of whether you think the Internet "kill switch" is constitutional or not, it is important to remember that "[t]rue patriots . . . realize one must protect the nation from all enemies, foreign and domestic, and that the essence of what it means to be patriotic is to protect our Constitution and its Bill of Rights with all of our might."[224]

224. ETZIONI, *supra* note 124, at 1.